IN THE CLAIMS:

1. (Cancelled)

2. (Cancelled)

3. (Cancelled)

4. (Cancelled)

5. (Cancelled)

6. (Cancelled)

7. (Previously Presented) A cryptographic device, compromising:

at least one data stream interceptor;

a main controller receiving input from said at least one data stream interceptor;

at least one data generating controller adapted to perform at least one data transfer protocol with at least one data generating device on command from said main controller;

at least one data storage controller adapted to perform at least one data transfer protocol with at least one data storage device on command from said main controller; and

at least one cipher engine adapted to transparently encrypt at least one data stream flowing between said at least one data generating device and said at least one data storage device on command from said main controller.

8. (Previously Presented) The cryptographic device of claim 7, wherein said at least one cipher engine is operatively coupled between at least one input buffer and at least one output buffer.

9. (Previously Presented) The cryptographic device of claim 8, wherein said at least one input buffer receives data from said at least one data generating device and said at least one data storage device.

10. (Previously Presented) The cryptographic device of claim 8, wherein said at least one output buffer outputs data to said at least one data generating device and said at least one data storage device.

11. (Previously Presented) A cryptographic device, comprising:

at least one data stream interceptor;

a main controller receiving input from said at least one data stream interceptor;

at least one data generating controller adapted to perform at least one data transfer protocol with at least one data generating device on command from said main controller;

at least one data storage controller adapted to perform at least one data transfer protocol with at least one data storage device on command from said main controller; and

at least one cipher engine adapted to transparently decrypt at least one data stream flowing between said at least one data generating device and said at least one data storage device on command from said main controller.

12. (Previously Presented) The cryptographic device of claim 11, wherein said at least one cipher engine is operatively coupled between at least one input buffer and at least one output buffer.

13. (Previously Presented) The cryptographic device of claim 12, wherein said at least one input buffer receives data input from said at least one data generating device and said at least one data storage device.

14. (Previously Presented) The cryptographic device of claim 12, wherein said at least one output buffer outputs data to said at least one data generating device and said at least one data storage device.

15. (Previously Presented) The cryptographic device, comprising:

at least one data stream interceptor;

a main controller receiving input from said at least one data stream interceptor;

at least one data generating controller adapted to perform at least one data transfer protocol with at least one data generating device on command from said main controller;

at least on data storage controller adapted to perform at least one data transfer protocol with at least one data storage device on command from said main controller; and

at least one cipher engine adapted to transparently encrypt and decrypt at least one data stream flowing between said at least one data generating device and said at least one data storage device on command from said main controller.

16. (Previously Presented) The cryptographic device of claim 15, wherein said at least one cipher engine is operatively coupled between at least one input buffer and at least one output buffer.

17. (Previously Presented) The cryptographic device of claim 16, wherein said at least one input buffer receives data from said at least one data generating device and said at least one data storage device.

18. (Previously Presented) The cryptographic device of claim 16, wherein said at least one output buffer outputs data to said at least one data generating device and said at least one data storage device.

19. (Previously Presented) A cryptographic device operatively coupled between a data generating device and a data storage device for use during data transfer, said cryptographic device comprising:

a data steam interceptor;

a main controller receiving input from said at least one data stream interceptor;

a data generating controller adapted to perform at least one data transfer protocol with the data generating device on command from said main controller;

a data storage controller adapted to perform at least one data transfer protocol with the data storage device on command from said main controller; and

a cipher engine adapted to transparently encrypt and decrypt at least one data stream flowing between the data generating device and the data storage device on command from said main controller.

20. (Previously Presented) A cryptographic device integrated within a data storage device for use during data transfer with a data generating device, said cryptographic device comprising:

a data stream interceptor;

a main controller receiving input from said data stream interceptor;

a data generating controller adapted to perform at least one data transfer protocol with the data generating device on command from said main controller;

a data storage controller adapted to perform at least one data transfer protocol with the data storage device on command from said main controller; and

a cipher engine adapted to transparently encrypt and decrypt at least one data stream flowing between the data generating device and the data storage device on command from said main controller.

21. (Previously Presented) A cryptographic device integrated within a data generating device for use during data transfer with a data storage device, said cryptographic device comprising:

a data stream interceptor;

a main controller receiving input from said data stream interceptor;

a data generating controller adapted to perform at least one data transfer protocol with the data generating device on command from said main controller;

a data storage controller adapted to perform at least one data transfer protocol with the data storage device on command from said main controller; and

a cipher engine adapted to transparently encrypt and decrypt at least one data stream flowing between the data generating device and the data storage device on command from said main controller.

22. (New) An apparatus comprising a data security apparatus configured to intercept data that is either transmitted from or to be received by a data processing apparatus, wherein:

intercepted data is either encrypted or decrypted or unchanged at the data security apparatus in accordance with a predetermined communication protocol; and

the data processing apparatus operates independently from the data security apparatus.

23. (New) The apparatus of claim 22, wherein the data security apparatus is configured to interface with a data storage apparatus.

24. (New) The apparatus of claim 23, wherein the intercepted data is transmitted from or to be received by the data storage apparatus.

25. (New) The apparatus of claim 23, wherein the data storage apparatus is selected from a group consisting of:

a hard disk apparatus;

a floppy disk apparatus;

a CD apparatus;

a magnetic tape apparatus;

a CD-RW apparatus;

a magnetic optical apparatus;

a digital video recorder;

a flash memory apparatus; and

a PCMCIA apparatus.

26. (New) The apparatus of claim 23, wherein the data storage apparatus is permanently coupled to the data security apparatus.

27. (New) The apparatus of claim 23, wherein the data storage apparatus is temporarily coupled to the data security apparatus.

28. (New) The apparatus of claim 22, wherein the data processing apparatus is a central processing unit.

29. (New) The apparatus of claim 28, wherein the central processing unit is comprised in a computing device, wherein the computing device is selected from a group consisting of:

a host computer;

a notebook;

a microprocessor;

a router; and

an interface card.

30. (New) The apparatus of claim 22, wherein the predetermined communication protocol is determined by a control signal from the data processing apparatus.

31. (New) The apparatus of claim 30, wherein the control signal is generated in the data processing apparatus for interpretation at a data storage apparatus.

32. (New) A method comprising intercepting data at a data security apparatus that is either transmitted from or to be received by a data processing apparatus, wherein:

intercepted data is either encrypted or decrypted or unchanged at the data security apparatus in accordance with a predetermined communication protocol; and

the data processing apparatus operates independently from the data security apparatus.